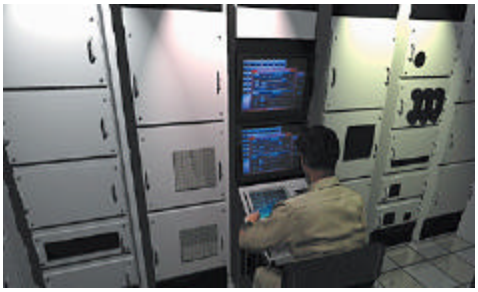
Navy Topic No: N99-167



PROMIA, Incorporated
160 Spear Street #320
San Francisco, CA 94105
http://www.promia.com

PROMIA is a leading developer and supplier of distributed object and component security tools, based on open standard components with advanced analytic capabilities. It's products are used in environments requiring high security, high reliability, high performance and scalability.

Since the early 1990's PROMIA has been in the forefront of developing software infrastructure solutions based on object-oriented technology and open standards for organizations worldwide.

PROMIA POC: John Mullen
415-536-1600
john.mullen@promia.com

Navy POC: Mike Weber
619-524-7333
michael.weber@navy.mil

SBIR Investment: $953K*****
Non-SBIR Investment: $8.3M

***** Includes Phase II Enhancement Funds

Intelligent Agent Security Module (IASM)

About the Technology

IASM is a high-speed secure distributed agent based system operating as a single analytical and statistical processor that connects agents gathering network information from many contractor and government off-the-shelf sources. IASM "watches" network traffic on many levels to determine misuse, fraud, or attack. Information is analyzed at the agent level, then normalized and fused as it is sent to multi-level IASM servers. The data is then correlated and analyzed further to determine cyber attack profiles in real time. Results are translated into simple English for Navy watch standers and centralized analysts to help them monitor the electronic terrain of their global networks.

Benefits to PEO C4I&Space and other DoD Programs

Since the mid to late 90's, the DoD has been subject to an exponential increase in computer-network system threats. Complex computer software, developed in rapidly changing commercial speed to market environments, has unintentionally introduced into user systems several computer-network vulnerabilities. The increasing ability of the cyber threat to exploit vulnerabilities and penetrate computer network systems undetected jeopardizes the war fighter's reliance on computer-network data availability and assurance in mission critical information. Network security administrators have had little ability to analyze the vast amount of cyber reconnaissance, intrusion, and attack data to qualify the security risk of an operational computer-network system. IASM gives the Navy an enterprise-wide security risk situation awareness view. For the first time analytic capabilities can accurately identify, source, and isolate cyber attacks.

Why IASM Provides Improved Security

- Reduces false positive network intrusion alerts to less than 1 percent
- Based on using an intrusion detection system alone, improves identification of network attacks by 64 percent
- Provides accurate and timely situation awareness with better forensic analysis, data reduction, graphic display reporting, and incident response
- Can detect novel non-signature attacks with cluster attack analysis and anomalous intrusion detection
- Reduces watch manning requirement by approximately 80 percent

Military and Commercial Significance

- Twenty advanced IASM systems are to be delivered to the Navy under a Phase III contract in 2001, eight shore systems in 2003, and 12 ship systems in 2004. Fleet activities and quantities are as follows:
  - Fleet Network Operating Centers (4)
  - Navy Component Task Force (1)
  - SPAWAR Systems Center Labs (3)
  - Aircraft carriers and Flag command ships (12)
- Commercial versions of the IASM product are available as a security internet appliance.